AntiVirus

AntiVirus uses a suite of integrated security technologies to provide against a variety of threats, including both known and unknown malicious codes (Malware), plus Advanced Targeted Attacks (ATA), also known as Advanced Persistent Threats (APT).

Advanced Protection against Malware and APTs

Malware and Advanced Persistent Threats can cause significant damages to today's organizations. These malicious codes are commonly designed to steal valuable data, gain unauthorized access, or cause products to degrade. FortiOS's AntiVirus is an industry-proven anti-malware security solution with robust features and deployment options.

FortiOS offers the unique ability to implement both Flow- and Proxy-based AV concurrently, depending on traffic type, users, and locations. Flow-based AV offers higher throughput performance while proxy-based solutions are useful in mitigating stealthy malicious codes. The AV detection capabilities are further enhanced with complementary security features and external sandbox integration.

By utilizing the unique Content Pattern Recognition Language (CPRL) built into the FortiASIC Content Processor, FortiOS is able to deliver high performance and low latency anti-malware capabilities. This real-time protection is backed by a team of worldwide researchers.

Key Features & Benefits

Robust feature set	Allows the flexibility to deploy appropriate protection according to security needs and infrastructure designs.
High performance utilizing FortiASIC and patented CPRL AV signatures.	Low latency and high capacity ensures that business applications are not affected while security is enforced.
Backed by FortiGuard Labs that deliver real-time protection	Critical digital assets are covered by continuous protection against latest threats.

Highlights

- Certification from multiple industries for best-in-class security and capacity with proven coverage and high performance.
- Multi-layered protection with extended AV components and external file analysis integration.
- Comprehensive remediation actions such as file quarantine and knowledge tools.

FEATURES

Industry's Validated Protection

FortiOS anti-malware components and FortiGuard AV signatures periodically undergo numerous authoritative certifications. These independent certifications demonstrate that the solution offered is of the highest standard in performance and accuracy, ensuring organizations are truly protected.

Fortinet has been consistently ranked among the top vendors for Virus Bulletin's RAP (Reactive And Proactive) bimonthly tests. This test measures a product's detection rates over the freshest samples available, as well as samples not seen until after product databases are frozen, thus reflecting both the vendor's ability to handle the huge quantity of newly emerging malware and accurately detect previously unknown malware.

Real Time Protection

The FortiGuard AntiVirus Service provides fully automated updates to ensure protection against the latest content-level threats via the experienced FortiGuard global network is backed by over 200 researchers.

FortiGuard AV service quick facts

- 95,000 malware programs neutralized per minute
- 1.8 Million new and updated AV definitions per week
- 190 TB of threat samples till date

Organizations can also engage the FortiGuard Premier Signature Service, which provides enhanced virus detection and threat analysis support. This service offers submissions for custom AntiVirus signatures on a daily basis, offering prioritized support with guaranteed response times.

Unique Proxy and Flow Based AV

FortiOS offers organizations the flexibility to select the most appropriate inspection method for different network sessions. This can be implemented by defining policies that match specific source objects (IP, IP ranges, users, and devices), destination objects, applications, and schedules with different AV profiles.

Flow-based AV relies on IPS technology where packets are inspected in real-time and matched against the AV signature database. It offers lower latency and higher throughput than Proxy-based AV. Flow-based AV is recommended for inspecting traffic that requires spontaneous user experience or when serving as an additional AV protection layer.

FortiOS's Proxy-based AV offers the most secure AV protection as it's able to inspect more protocols and provides replacement messages on wider range of applications.

AV Acceleration with Content Processor

The FortiASICS Content Processor (CP) accelerates content processing traditionally performed completely by the CPU. The CP reduces the resources required by the CPU when matching an incoming file against the signature database, thus improving system performance and stability.

Proactive Protection using Patented CPRL

Compact Pattern Recognition Language (CPRL) is a patented and proprietary programming language that allows for further inspection of common patterns to not only protect against threats and their variants but also to predict tomorrow's zero-day malware. It allows FortiGuard analysts to describe entire families of malware with a single program, instead of the traditional signature- based "one signature, one variant" model used by other vendors. With fewer signatures to match, throughput performance and latency naturally improve.

Intelligent Behavioral Evaluation

Signature-based security alone is no longer sufficient; it is now critical to understand how devices on your network are behaving. Threat Weight scoring provides a cumulative security ranking of each client device on your network based on a range of behaviors. It provides specific, actionable information that helps identify compromised systems and potential zero-day attacks in real-time.

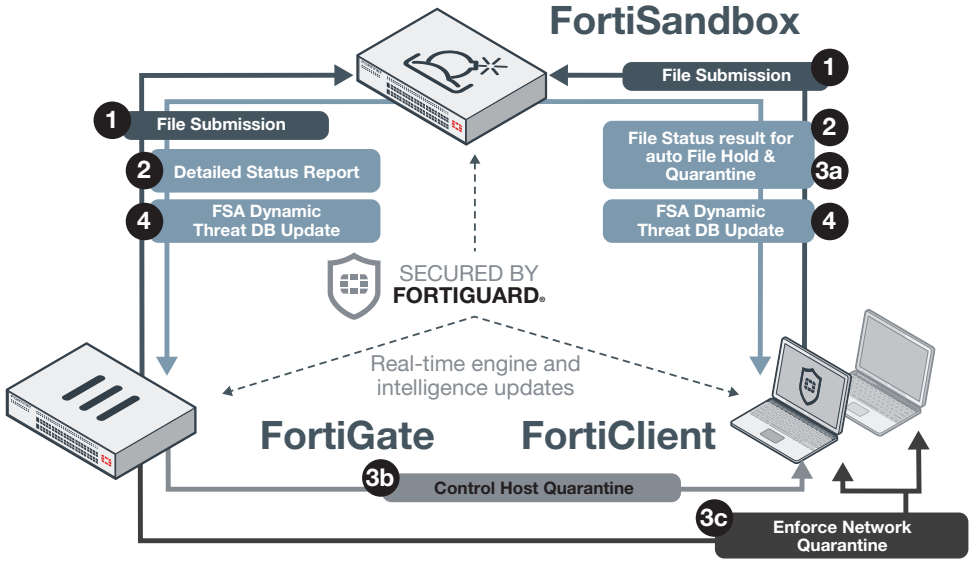
This unique system attaches predefined scores to various malicious network activities discovered by IPS, application control, URL filtering, etc., to determine the top suspicious users. Administrator can then further inspect these users to undercover unknown threats or APTs via FortiView.

FEATURES

External File Analysis Integration

FortiOS offers organizations the ability to adopt robust ATP (Advanced Threat Protection) framework that reaches mobile users and branch offices, detecting and preventing advanced attacks that may bypass traditional defenses by examining files from various vectors, including encrypted files. To detect unknown threats, zero-day, and targeted attacks, the FortiGate can engage external resources to perform additional file analysis. Files can be submitted to an on- premise appliance (FortiSandbox) or cloud-based service (FortiSandbox Cloud) after both proxy-based and flow- based AV processing.

It is also possible to configure the FortiGate to automatically receive dynamic signature updates from FortiSandbox and add the originating URL of any malicious file to a blocked URL list. In addition, if the organization deploys integrated endpoint control with FortiClient, an adminstrator can instruct an infected terminal to self-quarantine.



Query

1. File submission for Analysis
2. Respective analysis results are returned

Remediation

- 3a Auto File Quarantine on Host with option to hold file until result
- 3b Manual Host Quarantine by Admin
- 3c Manual Source IP Quarantine using Firewall

Protection

4. Proactive dynamic Threat DB update to gateway and host

FortiGate® - End-to-end Next Generation Firewall

- **Best Validated protection**
  FortiGate-based next generation firewall solutions are certified and validated by third-party authorities and programs such NSS Labs, ICSA, Virus Bulletin, and AV Comparatives for superior security effectiveness.
- **HIgh Speed and Flexible Connectivity**
  FortiGate appliances are powered by FortiASICs and designed on purpose-built integrated architecture that provides extremely high throughput and exceptionally low latency. They also offer variety of interfaces for today's network.
- **Broad Product Offerings**
  The FortiGate product family scales from desktop units for remote branch offices to high-end platforms for service providers and data centers while virtualized appliances support a wide range of hypervisors and public cloud infarstructure.

FEATURES

File Filtering

File filtering using data leak prevention (DLP) on the FortiGate offers an effective ways to stop unwanted file transmission instantly. Administrators may implement granular file controls by defining protection profiles using filenames or nearly 50 different file types over mail, web, and file download protocols.

File Quarantine

FortiOS offers sophisticated file quarantine capabilities that allow organizations to archive suspicious or blocked files for further examination or to release false positives.

Anti-bot

Organizations may prevent, uncover, and block botnet activities using FortiOS Anti-Bot traffic pattern detection and domain and IP reputation services supplied in real-time by FortiGuard threat experts.

User Notification

User notifications are helpful in reducing administration and support burdens, as well as providing user education. FortiOS is able to automatically replace blocked attachments and downloads with detailed information sent to E-mail, FTP, or web users.

Monitoring, Log & Reporting

FortiOS empowers organizations to implement security best practices that require continuous examination of their threat status and adaptation to new requirements. The FortiView widgets provide useful analysis data with detailed and contextual session information, which can be filtered, ranked, and –further inspected. System events can also be archived via logs, which in turn can generate useful trending and overview reports.

FortiOS also offers robust in-built E-mail and SMS alert systems, as well as integration with external threat management systems using SNMP and standard-based syslogs.

ADDITIONAL REFERENCE

Resource	URL
FortiOS Handbook - The Complete Guide	http://docs.fortinet.com/fortigate/admin-guides
Fortinet Knowledge Base	http://kb.fortinet.com/
FortiGate Product Page	https://www.fortinet.com/products-services/products/firewall.html

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne 06560
Alpes-Maritimes, France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6395.2788

LATIN AMERICA SALES OFFICE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
United States
Tel: +1.954.368.9990

FST-PROD-DS-GT15K

INSIDE-AV-DAT-R2-201608